International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, July-December 2022, Submitted in December 2022, iajesm2014@gmail.com

Data Integrity and Meeting the Regulatory Expectations

Kamaraj A, Research Scholar, Sunrise University, Alwar, Rajasthan, India
Adkar Prafulla Prakash, Research Guide, Sunrise University, Alwar, Rajasthan, India

Abstract

Many Companies continue to struggle with basic data integrity problems. This is evident from the number of warning letters and Form 483 inspectional observations at manufacturing sites around the world. Non-compliance can lead to product seizures, product non-approvals or delays of approvals, import restrictions, substantial fines, disbarment, and criminal liability for individuals or company. Data integrity errors can erode the trust with customers and FDA. Even an innocent mistake can be perceived as an intentional fraud. This article guides FDA regulated companies through the data integrity compliance process. Data integrity is an important current issue for regulators around the world. During inspections a multitude of problems being found by the pharmaceutical regulatory agency because poor practices develop the substandard product for patients. Collection of various types of information and results collectively made in the form of data. This data becomes one of the most valuable assets of any organization but without integrity, this data is not much useful. Accuracy and original data increase the chances of stability and performance of an organization. Data integrity is the extent to which all data are complete, consistent and accurate throughout the life cycle of data. It includes Good Documentation Practice which leads to preventing data from being altered, copied or moved. In data integrity, data means all original records including source data and metadata which may be recorded in paper or electronic form. To assure the data integrity many regulatory bodies such as USFDA, Health Canada, and EMEA recommended the use of ALCOA (Attributable, Legible, Contemporaneous, Original and Accurate).

Keywords: Data integrity, ALCOA, regulatory body, USFDA, Health Canada, and EMEA

Introduction

Data integrity means that the data is accurate and reliable. The data quality is referred to as "Data Integrity." It is maintaining and assuring the accuracy and consistency of data over its entire life-cycle. Research and processing Information collected and resulting in an increasing amount and varied types of data being collected. This data is very important, but without integrity, this data not have much value.[1]. Data is information that has been translated into a form that is efficient for movement or processing, It has become one of the most valuable assets of any company project or research. The better data integrity a company has, the more ethically successful it is likely to become growth. Poor data integrity practices and vulnerabilities undermine the quality of records and evidence and may ultimately undermine the quality of medicinal products. Data integrity applies to all elements of the Quality Management System and the principles herein apply equally to data generated by electronic and paper-based systems. The responsibility for good practices regarding data management and integrity lies with the manufacturer or distributor undergoing inspection. They have full responsibility and a duty to assess their data management systems for potential vulnerabilities and take steps to design and implement good data governance practices to ensure data integrityis maintained.

Data integrity is the issue of maintaining and ensuring the accuracy and consistency of data over its lifecycle. This includes good documentation practice, good data management practices, such as preventing data from being altered each time it is copied or moved. Data integrity applies to both paper records and electronic records. Processes and procedures are putin place for companies to maintain data integrity during normal operation .

As per MHRA, GMP data integrity guidance for industry March 2015. Data Integrity is defined as "the extent to which all data are complete, consistent and accurate, throughout the data lifecycle" and is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality.

The word integrity evolved from the Latin adjective integer, meaning whole or complete [2]. Integrity is the qualifications of being honest and having strong moral principles; moral uprightness. It is generally a personal choice to hold oneself to consistent moral and ethical

standards[3]. In ethics, integrity is regarded by many as the honesty and truthfulness or accuracy of one's actions. Integrity can stand in opposition to hypocrisy. It's the inner sense of "wholeness" deriving from qualities such as honesty and consistency of character.

The regulatory requirements for data integrity[4-6]

- 21 CFR 211 and 212 : Requirements with respect to data integrity include, among other things:
  - "Backup data are exact and complete", and "secure from alteration, inadvertent erasures, or loss"
  - Data be "stored to prevent deterioration or loss"
  - Certain activities be "documented at the time of performance" and that laboratory controls be "scientifically sound"
  - records be retained as "original records", "true copies", or other "accurate reproductions of the original records"
  - "complete information", "complete data derived from all tests", "complete record of all data", and "complete records of all tests performed"
- Electronic signature and record-keeping requirements
- FDA Draft Guidance, Data Integrity and Compliance with cGMP - April 2016: This guidance provides the Agency's current thinking on the creation and handling of data in accordance with CGMP requirements.
- MHRA GMP Data Integrity Definitions and Guidance for Industry - March 2015
- PDA code of Conduct

Causes of Data Integrity Violations and Challenges

Despite the many guidance documents and public statements that explain what is expected of the manufacturers, many companies struggle with data integrity deficiencies due to the following reasons:

The Pharmaceutical industry data is largely collected manually. There are multiple data transfer points such as data from notebooks/worksheets to calculators and back, data from worksheets/notebooks to LIMS, worksheets/notebooks to reports etc. Errors can occur during data transfer as frequently observed during audits.

The management must play a pivotal role by taking steps to offset each of the above factors that cause data integrity deficiencies.

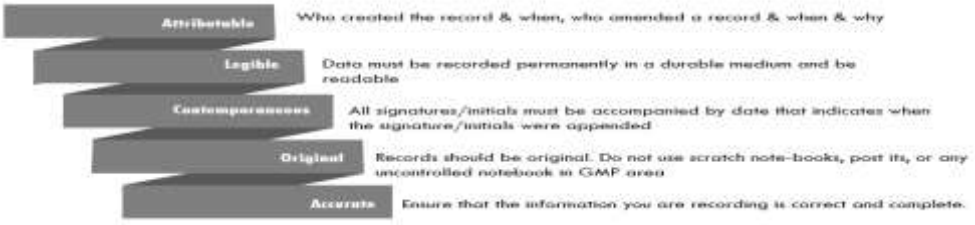
An important step on the path to data integrity compliance is to understand associated definitions and implement the best practices given in the guidance documents.

Data Integrity Associated Definitions and Best Practices

Data Integrity

'Data integrity refers to the completeness, consistency, and accuracy of data. Such data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).'

ALCOA Best practice in data integrity



Metadata

- Metadata is the contextual information required to understand data.
- It is described as data about data.
- It is the structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data.
- Among other things, metadata for a particular piece of data could include
  - Date/time stamp for when the data were acquired
  - User ID of the person who conducted the test or analysis that generated the data
  - Instrument ID used to acquire data
  - Audit trials

Audit Trial

- A secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record.
- An audit trail is a chronology of the "who, what, when, and why" of a record.

Static and Dynamic data:

- **Static Data:** Data record that does not change such as a paper record or an electronic image
- **Dynamic Data:** Data record that allows interaction between user and the record. For example, a chromatographic record which allows user to change the baseline and reprocess.

Backup

A true copy of the original data that is maintained securely throughout the records retention period. The backup file should contain the data (which includes associated metadata) and should be in the original format or in a format compatible with the original format.

Best Practices for Achieving Data Integrity

Impart Training, create awareness

Personnel in every process on the manufacturing floor must be trained in proper data management. The training must go beyond good document practices. It should cover why the process are conducted the way they are. To enhance the training, include:

- Consequences of poor handling for any given process
- How the smallest of mistakes evolve into serious problems
- Why validations are important
- Why protocols should be followed

Set Controls on Human errors Procedures, and technology[7-10]

- Have SOPs that are well-defined, clear, and simple. Train staff adequately on them.
- Keep audit trials in order to clearly show who accesses a given system, which login credentials were used and the date and time it was accessed. This will help investigate issues and address root cause.
- Regularly review audit trials
- Keep records of audits at handy to show investigators that reviews are being conducted routinely by trained professionals
- Ensure your SOPS offer a process for escalating issues to management should they be discovered
- Simplify SOPs, train staff on all directives, and monitor the effectiveness of these efforts

Set Procedural controls

- Embed procedural and administrative controls in your core business activity. It should consist of a suit of documents that include written directives, training programs, record and review management, audits and self-inspections of governing processes.

Set Technical controls

- Set controls to protect information systems such as passwords, access controls for operating systems or application software programs, network protocols, firewalls and intrusion detection systems, encryption technology, network traffic flow regulators, etc.

- Set appropriate technical controls into products for all three stages namely a) data at rest b) data in motion c) data in use.
- Create a culture of integrity
- Recognize the contributions of employees and encourage them to be critical, and divergent thinkers.

Set Document controls

Data must not be recorded in unofficial forms, writing pads, and uncontrolled media. This policy must be stated in the SOPs for good documentation practices. (see B'B' 211.100, 213 211.160(a), 211.186, 212.20(d), and 212.60(g))

- Lab notebooks, worksheets should be issued by the quality unit.
- System user accounts especially those with data alteration abilities should not be shared
- Limit duplication risks such as duplicate copies of paper records, multiple copies of databases/spreadsheets and so on by maintaining a centralized library
- Audit electronic systems, ensure verifying controls are in place and functioning
- Ensure that archiving processes maintain and protect data loss
- Backup electronic data regularly, maintain as per procedural GMP requirements.
- Draw a single line through the erroneous entry. Record correct entry, initial and date providing reason for the correction. Justify and document any data discarding. B'B' 211.192, 211.194, 212.50(a), and 212.70(f)(1)(vi))
- Perform data entry accurately, truthfully and completely
- Store data, documents and backups securely during their retention periods. Limit access and use fireproof storage as necessary.

Management Responsibility[11-15]: It is common observation management using 'Rule by Fear' method with employees (for example- employee do what employer are told him). This leads to a culture of fear and blame and an inability of employees to challenge and not follow regulatory guidelines.

- Poor education could lead to bad decisions or inappropriate behaviour based on knowing 'How' but not 'Why Complex systems and systems with inappropriate design can encourage and, at times, even force bad practices.
- An employee should be encouraged to take advantage of an open-door route to organization top management when it comes to raising compliance issues and discussing potential compliance concerns pertaining to datareliability [10].

Common Data Integrity Issues

- **User privileges:** The system configuration for the software does not adequately define or segregate user levels and users have access to inappropriate software privileges such as modification of methods and integration.
- **Common passwords**: Where analysts share passwords, it is not possible to identify who creates or changes records,thus the A in ALCOA is not clear.
- **Computer system control:** Laboratories have failed to implement adequate controls over data, and unauthorized access to modify, delete, or not save electronic files is not prevented; the file, therefore, may not be original, accurate, or complete. [1]
- **Audit Trail capture:** FDA recommends that audit trails capturing changes to critical data be reviewed with each record and before final approval of the record.
- Audit trails subject to regular review should include, for example, changes to finished product test results, sample run sequences, sample identification, critical process parameters [12].
- Overwriting
- Runs that have been aborted
- Testing into compliance
- Deleting data
- Backdating
- Altering data

The reason of issue: There is various reason for data integrity issue some of them write the following:

1. No raw data to support records or loss of data duringchanges to the system
2. Creating inaccurate and incomplete records
3. Test results for one batch used to release other batches

4. Backdating
5. Discarding data repeated tests, trial runs, sample runs(testing into compliance)
6. Changing integration parameters of chromatography data to obtain passing results
7. Deletion/manipulation of electronic records or fabricatingof data
8. Turning off audit trail
9. Sharing password
10. Inadequate controls for access privileges
11. Inadequate/incomplete computer validation.
12. Activities not recorded contemporaneously
13. Employees that sign that they completed manufacturing steps when the employees were not on premises at the time the steps were completed

Difference between data security and dataintegrity

Data Security	Data Integrity
Data security defines the prevention of data corruption through the use of controlled access mechanisms.	Data integrity defines data quality, which ensures that the data is complete and is a complete design.
Data security deals with the protection of data.	Data integrity deals with the validity of data.
Data security is making sure only the people who should have access to the data are the only ones who can access the data.	Data integrity is making sure the data is correct and not corrupt.
Data security refers to making sure that data is accessed by its intended users, thus ensuring the privacy and protection of data.	Data integrity refers to the structure of the data and how it matches the schema of the database.
Authentication/authorization, encryptions and masking are some of the popular means of data security.	Backing up, designing a suitable user interface and error detection/correction in data are some of the means to preserve integrity.
For example, if you have an account in the “yahoo.com”, then you have to give your correct username and password to access your account or e mail. Similarly, when you insert your ATM card into the Automated Teller Machine (ATM), the machine reads your ID number printed on the card and then asks you toenter your pin code (or password). In this way, you can access your account.	For example, a balance for any account must not be less than zero. Such constraints are enforced in the system by adding appropriate code in application programs. But, when new constraints are added, such as balance should not be less than Rs. 5000, application programs need to be changed. But, it is not an easy task to change programs whenever required.

Conclusion:

In the pharmaceutical industry, data integrity play an important role to maintain the quality of a final product because the poor practice can allow the substandard product to reach patients, so it’s necessary for an existing system to ensure the data integrity, data traceability, and reliability. On quality bases, data integrity is a critical component of a Quality System. Quality data provides the base for the confidence of the company to utilize correct data to operate inaccordance with regulatory requirements.

Data integrity is critically important to regulators for various reasons, including patient safety, process, and product quality. The integrity and trustworthiness of the data provide a baseline for the regulators' opinion about the company.

It’s also the responsibility of the manufacturer to prevent and detect poor data integrity practices which occur due to the lack of quality system effectiveness. Quality Risk Management (QRM) approach can prevent, detect and control potential risks where data is

generated and used to make manufacturing and quality decisions, ensure it is trustworthy and reliable.

References:

1. Data Integrity in the Analytical Laboratory. PharmaTech.com Advance Devlopment and Manufacturing.02 May 2014. http://www.pharmtech. com/data-integrity-analytical-laboratory
2. Dorkin R. Law's Empire Harvard University Press, 1987, 191.
3. Intgrity. Doing the right thing for the right reason, McGill-Queen's University Press, 2010, 25.
4. Ankur C. ALCOA in Pharmaceuticals: a necessary tool for quality. Pharmaceuticals Guidelines. Cited, 2018. https://www.qiksolve.com/defining-data-integrity-alcoa/
5. MHRA. GMP Data Integrity Definitions and Guidance for Industry Revision, 2015.
6. Review of Good Data Integrity Principles Of ni system, 808 Salem Woods Drive Suite, 103:1-11. http://www. ofnisystems.com/media/Data_Integrity_Article.pdf
7. World Health Organization, Guidance on good data and record management practices, 2016. http://www.who.int/ medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf
8. Guidance on good data and record management practices, WHO Technical Report Series. 2016; 5:165- 209
9. World Health Organization, Guidance on good data and record management practices, ('Draft for comment), 2015.
10. Review of Good Data Integrity Principles, Ofni Systems,1-11
11. McDowall RD, LCGC Europe, RD McDowall Ltd, UK. 2017; 30(2):84-87.
12. Sharon K. Pederson (PharmD National Expert of Pharmaceutical Inspections Food and Drug Administration). Data Integrity Issues & Concerns PDA Meeting St. Louis, MO, 2017. ISBN 9780773582804. 2nd edition, writer, Barbara Killinger, 2013.
13. Pharmaceutical manufacturing. By Ashley Ruth, Senior Consultant, Analytical Services, Bio Tech Logic, Inc,2017.
14. US Food and Drug Administration, Code of Federal Regulations - Title 21 - Food and Drugs, Medical Device Databases, 2018. https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Databases/ucm135680.htm
15. Stephen Hart, Data Integrity TGA Expectations, PDA conference, 2015.